



# CheckPoint

**156-115.77 Exam**

**Check Point Certified Security Master**

**Thank you for Downloading 156-115.77 exam PDF Demo**

**You can also Buy Latest 156-115.77 Exam Full Version**

<https://www.certkillers.net/Exam/156-115.77>

<https://www.certkillers.net>

---

**Question: 1**

---

What command would you use for a packet capture on an absolute position for TCP streaming (out) 1ffffe0

- A. fw ctl chain -po 1ffffe0 -o monitor.out
- B. fw monitor -po -0x1ffffe0 -o monitor.out
- C. fw monitor -e 0x1ffffe0 -o monitor.out
- D. fw monitor -pr 1ffffe0 -o monitor.out

---

**Answer: B**

---

---

**Question: 2**

---

The command fw monitor -p all displays what type of information?

- A. It captures all points of the chain as the packet goes through the firewall kernel.
- B. This is not a valid command.
- C. The -p is used to resolve MAC address in the firewall capture.
- D. It does a firewall monitor capture on all interfaces.

---

**Answer: A**

---

---

**Question: 3**

---

What does the IP Options Strip represent under the fw chain output?

- A. IP Options Strip is not a valid fw chain output.
- B. The IP Options Strip removes the IP header of the packet prior to be passed to the other kernel functions.
- C. The IP Options Strip copies the header details to forward the details for further IPS inspections.
- D. IP Options Strip is only used when VPN is involved.

---

**Answer: B**

---

---

**Question: 4**

---

The command that lists the firewall kernel modules on a Security Gateway is:

- A. fw list kernel modules
- B. fw ctl kernel chain
- C. fw ctl debug -m
- D. fw list modules

---

**Answer: C**

---

---

**Question: 5**

---

Which of the following BEST describes the command fw ctl chain function?

- A. View how CoreXL is distributing traffic among the firewall kernel instances.
- B. View established connections in the connections table.
- C. View the inbound and outbound kernel modules and the order in which they are applied.
- D. Determine if VPN Security Associations are being established.

---

**Answer: C**

---

---

**Question: 6**

---

The command \_\_\_\_\_ shows which firewall chain modules are active on a gateway.

- A. fw stat
- B. fw ctl debug
- C. fw ctl chain
- D. fw ctl multik stat

---

**Answer: C**

---

---

**Question: 7**

---

The command fw ctl kdebug <params> is used to:

- A. list enabled debug parameters.
- B. read the kernel debug buffer to obtain debug messages.
- C. enable kernel debugging.
- D. select specific kernel modules for debugging.

---

**Answer: B**

---

---

**Question: 8**

---

Compare these two images to establish which blade/feature was disabled on the firewall.



## Before

```
[Expert@fw1:0]# fw ctl chain
in chain (16):
 0: -7f800000 (c26a9c70) (ffffffff) IP Options Strip (in) (ipopt_strip)
 1: - 20000000 (c183b020) (00000003) vpn decrypt (vpn)
 2: - 1fffff8 (c1846080) (00000001) l2tp inbound (l2tp)
 3: - 1fffff6 (c26ab420) (00000001) Stateless verifications (in) (asm)
 4: - 1fffff2 (c1862a60) (00000003) vpn tagging inbound (tagging)
 5: - 1fffff1 (c1838700) (00000003) vpn decrypt verify (vpn_ver)
 6: - 10000000 (c2728940) (00000003) SecureXL conn sync (secxl_sync)
 7:   0 (c2654220) (00000001) fw VM inbound (fw)
 8:   1 (c26cb2b0) (00000002) wire VM inbound (wire_vm)
 9:  20000000 (c1839b90) (00000003) vpn policy inbound (vpn_pol)
10: 10000000 (c1726e40) (00000003) SecureXL inbound (secxl)
11: 7f600000 (c269f2b0) (00000001) fw SCV inbound (scv)
12: 7f730000 (c2835210) (00000001) passive streaming (in) (pass_str)
13: 7f750000 (c2a2b3f0) (00000001) TCP streaming (in) (cpas)
14: 7f800000 (c26aa010) (ffffffff) IP Options Restore (in) (ipopt_res)
15: 7fb00000 (c2db29f0) (00000001) HA Forwarding (ha_for)

out chain (14):
 0: -7f800000 (c26a9c70) (ffffffff) IP Options Strip (out) (ipopt_strip)
 1: - 1fffff7 (c1837e0) (00000003) vpn nat outbound (vpn_nat)
 2: - 1fffff0 (c2a2b270) (00000001) TCP streaming (out) (cpas)
 3: - 1fffff5 (c2835210) (00000001) passive streaming (out) (pass_str)
 4: - 1ff00000 (c1862a60) (00000003) vpn tagging outbound (tagging)
 5: - 1f000000 (c26ab420) (00000001) Stateless verifications (out) (asm)
 6:   0 (c2654220) (00000001) fw VM outbound (fw)
 7:   1 (c26cb2b0) (00000002) wire VM outbound (wire_vm)
 8:  20000000 (c18381e0) (00000003) vpn policy outbound (vpn_pol)
 9: 10000000 (c2726e40) (00000003) SecureXL outbound (secxl)
10: 1fffff0 (c1846c30) (00000001) l2tp outbound (l2tp)
11: 20000000 (c183ba0) (00000003) vpn encrypt (vpn)
12: 7f700000 (c2azd840) (00000001) TCP streaming post VM (cpas)
13: 7f800000 (c26aa010) (ffffffff) IP Options Restore (out) (ipopt_res)
```

## After

```
[Expert@fw1:0]# fw ctl chain
in chain (11):
 0: -7f800000 (c26a9c70) (ffffffff) IP Options Strip (in) (ipopt_strip)
 1: - 1fffff6 (c26ab420) (00000001) Stateless verifications (in) (asm)
 2: - 10000000 (c2728940) (00000003) SecureXL conn sync (secxl_sync)
 3:   0 (c2654220) (00000001) fw VM inbound (fw)
 4:   1 (c26cb2b0) (00000002) wire VM inbound (wire_vm)
 5:  10000000 (c2726e40) (00000003) SecureXL inbound (secxl)
 6:  7f600000 (c269f2b0) (00000001) fw SCV inbound (scv)
 7:  7f730000 (c2835210) (00000001) passive streaming (in) (pass_str)
 8:  7f750000 (c2a2b3f0) (00000001) TCP streaming (in) (cpas)
 9:  7f800000 (c26aa010) (ffffffff) IP Options Restore (in) (ipopt_res)
10:  7fb00000 (c2db29f0) (00000001) HA Forwarding (ha_for)

out chain (9):
 0: -7f800000 (c26a9c70) (ffffffff) IP Options Strip (out) (ipopt_strip)
 1: - 1fffff0 (c2a2b270) (00000001) TCP streaming (out) (cpas)
 2: - 1fffff0 (c2835210) (00000001) passive streaming (out) (pass_str)
 3: - 1f000000 (c26ab420) (00000001) Stateless verifications (out) (asm)
 4:   0 (c2654220) (00000001) fw VM outbound (fw)
 5:   1 (c26cb2b0) (00000002) wire VM outbound (wire_vm)
 6:  10000000 (c2726e40) (00000003) SecureXL outbound (secxl)
 7:  7f700000 (c2a2d840) (00000001) TCP streaming post VM (cpas)
 8:  7f800000 (c26aa010) (ffffffff) IP Options Restore (out) (ipopt_res)
```

©2014 Check Point Software Technologies Ltd.

1

- A. IPS
- B. VPN
- C. NAT
- D. L2TP

## Answer: B

### Question: 9

What command would give you a summary of all the tables available to the firewall kernel?

- A. fw tab
- B. fw tab -s
- C. fw tab -h
- D. fw tab -o

## Answer: B

### Question: 10

What flag option(s) must be used to dump the complete table in friendly format, assuming there are more than one hundred connections in the table?

- A. fw tab -t connections -f
- B. fw tab -t connect -f -u
- C. fw tab -t connections -s

D. fw tab -t connections -f -u

---

**Answer: B**

---

### **Question: 11**

Which directory below contains the URL Filtering engine update info? Here you can also go to see the status of the URL Filtering and Application Control updates.

- A. \$FWDIR/urlf/update
- B. \$FWDIR/appi/update
- C. \$FWDIR/appi/urlf
- D. \$FWDIR/update/appi

---

**Answer: B**

---

### **Question: 12**

For URL Filtering in the Cloud in R75 and above, what table is used to contain the URL Filtering cache values?

- A. urlf\_blade\_on\_gw
- B. urlf\_cache\_tbl
- C. urlf\_cache\_table
- D. url\_scheme\_tab

---

**Answer: C**

---

### **Question: 13**

You are troubleshooting a Security Gateway, attempting to determine which chain is causing a problem. What command would you use to show all the chains through which traffic passed?

- A. [Expert@HostName]# fw ctl chain
- B. [Expert@HostName]# fw monitor -e "accept;" -p all
- C. [Expert@HostName]# fw ctl debug -m
- D. [Expert@HostName]# fw ctl zdebug all

---

**Answer: B**

---

### **Question: 14**

True or False: Software blades perform their inspection primarily through the kernel chain modules.

- A. False. Software blades do not pass through the chain modules.
- B. True. Many software blades have their own dedicated kernel chain module for inspection.

- C. True. All software blades are inspected by the IP Options chain module.
- D. True. Most software blades are inspected by the TCP streaming or Passive Streaming chain module.

---

**Answer: B**

---

**Question: 15**

---

When using the command fw monitor, what command ensures the capture is accurate?

- A. export TDERROR\_ALL\_ALL=5
- B. fwaccel off
- C. fwaccel on
- D. fw accel off

---

**Answer: B**

---

**Thank You for trying 156-115.77 PDF Demo**

To Buy Latest 156-115.77 Exam Full Version visit link below

<https://www.certkillers.net/Exam/156-115.77>

## Start Your 156-115.77 Preparation

**[Limited Time Offer]** Use Coupon “CKNET” for further discount on your purchase. Test your 156-115.77 preparation with actual exam questions.

<https://www.certkillers.net>